

1 Frank S. Hedin (SBN 291289)
2 Hedin LLP
3 535 Mission Street, 14th Floor
4 San Francisco, CA 94105
5 Telephone: (305) 357-2107
6 Facsimile: (305) 200-8801
7 E-Mail: fhedin@hedinllp.com

Attorney for Plaintiffs and the Putative Class

8
9
10 **UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

11 MICHAEL ARCHER and DYLAN
12 MACALUSO, individually and on
13 behalf of all others similarly situated,

14 Plaintiff,

15 v.

16 SHOUT! FACTORY, LLC

17 Defendant.
18
19
20

Case No. 2:24-cv-7056

**CLASS ACTION
COMPLAINT DEMAND
FOR JURY TRIAL**

**ACTION SEEKING
NATIONWIDE RELIEF**

21 Plaintiff Michael Archer (“Plaintiff Archer”) and Plaintiff Dylan
22 Macaluso (“Plaintiff Macaluso”) (collectively, “Plaintiffs”), individually and
23 on behalf of all others similarly situated, make the following allegations
24 pursuant to the investigation of counsel and based upon information and
25
26
27
28

1 belief, except as to allegations pertaining specifically to themselves or their
2
3 counsel, which are based on personal knowledge.

4 NATURE OF THE CASE

5 1. Plaintiffs bring this action for legal and equitable remedies to
6
7 redress and put a stop to Defendant Shout! Factory, LLC's practices of
8
9 knowingly selling, transmitting, and/or otherwise disclosing, to various
10
11 third parties, records containing the personal information of each of their
12
13 customers, along with detailed information revealing the titles and subject
14
15 matter of the videos and other audiovisual materials purchased by each
16
17 customer (collectively "Personal Viewing Information") in violation of the
18
19 Video Privacy Protection Act, 18 U.S.C. §2701et. seq. ("VPPA").
20

21 2. Over the past two years, Defendant has systematically
22
23 transmitted (and continues to transmit today) its customers' Personal
24
25 Viewing Information to Meta using a snippet of programming code called
26
27 the "Meta Pixel," which Defendant chose to install on its shoutfactory.com
28
and other websites.

3 3. The information Defendant disclosed (and continues to disclose)
4
5 to Meta, via the Meta Pixel it installed on its websites, includes the
6
7 customer's Facebook ID ("FID") coupled with the title of each of the specific
8
9

1 videos that the customer purchased on Defendant's websites. A customer's
2 FID is a unique sequence of numbers linked to the Meta profile belonging
3 to that customer. The customer's Meta profile, in turn, publicly identifies
4 the customer by name (and contains other personally identifying
5 information about the customer as well). Entering "facebook.com/[FID]"
6 into a web browser returns the Meta profile of the person to whom the FID
7 corresponds. Thus, the FID identifies a person more precisely than a name,
8 as numerous persons may share the same name but each person's Facebook
9 profile (and associated FID) uniquely identifies one and only one person. In
10 the simplest terms, the Meta Pixel installed by Defendant captures and
11 discloses to Meta information that reveals the specific videos that a
12 particular person purchased from Defendant's websites (hereinafter,
13 "Private Viewing Information").

14
15 4. Defendant disclosed and continues to disclose its customers'
16 Private Viewing Information to Meta without asking for let alone obtaining
17 its customers' consent to these practices.

18
19 5. The VPPA clearly prohibits what Defendant has done.
20 Subsection (b)(1) of the VPPA provides that, absent the consumer's prior
21 informed, written consent, any "video tape service provider who knowingly
22
23
24
25
26
27
28

1 discloses, to any person, personally identifiable information concerning any
2 consumer of such provider shall be liable to the aggrieved person for,” 18
3 U.S.C. § 2710(b)(1), *inter alia*, liquidated damages in the amount of
4 \$2,500.00 per violation and equitable relief, *see id.* § 2710(c).
5

6
7 6. Accordingly, on behalf of themselves and the putative Class
8 members defined below, Plaintiffs bring this Class Action Complaint
9 against Defendant for intentionally and unlawfully disclosing their
10 Personal Viewing Information to Meta.
11

12 PARTIES

13 I. Plaintiff Archer

14
15 7. Plaintiff Archer is, and at all times relevant hereto was, a citizen
16 and resident of Metairie, Louisiana.
17

18 8. Plaintiff Archer is, and at all times relevant hereto was, a user
19 of Meta.
20

21 9. On or about May 7, 2024, Plaintiff Archer purchased
22 prerecorded video material from Defendant by requesting and paying for
23 such material on Defendant’s website, www.shoutfactory.com, and by
24 providing his name, email address, and home address for shipment of such
25 material. Accordingly, Plaintiff Archer requested or obtained, and is
26
27
28

1 therefore a consumer of, prerecorded video material sold by Defendant on
2 its website.
3

4 10. At all times relevant hereto, including when purchasing
5 prerecorded video material from Defendant on its website, Plaintiff Archer
6 had a Meta account, a Meta profile, and an FID associated with such profile.
7

8 11. When Plaintiff Archer purchased prerecorded video material
9 from Defendant on its website, Defendant disclosed to Meta Plaintiff
10 Archer's FID coupled with the specific title of the video he purchased (as
11 well as the URL where such video is available for purchase), among other
12 information concerning Plaintiff Archer and the device on which he used to
13 make the purchase.
14
15

16 12. Plaintiff Archer has never consented, agreed, authorized, or
17 otherwise permitted Defendant to disclose his Personal Viewing
18 Information to Meta. In fact, Defendant never even provided Plaintiff
19 Archer with written notice of its practices of disclosing its customers'
20 Personal Viewing Information to third parties such as Meta.
21
22

23 13. Because Defendant disclosed Plaintiff Archer's Private Viewing
24 Information (including his FID, the title of the prerecorded video material
25 he purchased from Defendant's website, and the URL where such video is
26
27
28

1 available for purchase) to Meta during the applicable statutory period,
2 Defendant violated Plaintiff Archer's rights under the VPPA and invaded
3 his statutorily conferred interest in keeping such information (which bears
4 on his personal affairs and concerns) private.
5

6 **II. Plaintiff Macaluso**

7
8 14. Plaintiff Macaluso is, and at all times relevant hereto was, a
9 citizen and resident of Cleveland, Ohio.
10

11 15. Plaintiff Macaluso is, and at all times relevant hereto was, a
12 user of Meta.
13

14 16. On or about March 4, 2024, Plaintiff Macaluso purchased
15 prerecorded video material from Defendant by requesting and paying for
16 such material on Defendant's website, www.shoutfactory.com, and by
17 providing his name, email address, and home address for shipment of such
18 material. Accordingly, Plaintiff Macaluso requested or obtained, and is
19 therefore a consumer of, prerecorded video material sold by Defendant on
20 its website.
21
22

23 17. At all times relevant hereto, including when purchasing
24 prerecorded video material from Defendant on its website, Plaintiff
25 Macaluso had a Meta account, a Meta profile, and an FID associated with
26
27
28

1 such profile.

2
3 18. When Plaintiff Macaluso purchased prerecorded video material
4 from Defendant on its website, Defendant disclosed to Meta Plaintiff
5 Macaluso's FID coupled with the specific title of the video he purchased (as
6 well as the URL where such video is available for purchase), among other
7 information concerning Plaintiff Macaluso and the device on which he used
8 to make the purchase.
9
10

11 19. Plaintiff Macaluso has never consented, agreed, authorized, or
12 otherwise permitted Defendant to disclose his Personal Viewing
13 Information to Meta. In fact, Defendant never even provided Plaintiff
14 Macaluso with written notice of its practices of disclosing its customers'
15 Personal Viewing Information to third parties such as Meta.
16
17

18 20. Because Defendant disclosed Plaintiff Macaluso's Private
19 Viewing Information (including his FID, the title of the prerecorded video
20 material he purchased from Defendant's website, and the URL where such
21 video is available for purchase) to Meta during the applicable statutory
22 period, Defendant violated Plaintiff Macaluso's rights under the VPPA and
23 invaded his statutorily conferred interest in keeping such information
24 (which bears on his personal affairs and concerns) private.
25
26
27
28

1 **III. Defendant Shout! Factory, LLC**

2 21. Defendant is a Delaware limited liability company with its
3 headquarters and principal place of business located at 1640 S. Sepulveda
4 Blvd., Suite 400, Los Angeles, CA 90025.

5
6 22. Defendant operates and maintains the websites
7 www.shoutfactory.com and www.ghiblicollection.com, among others, where
8 it is engaged in the business of selling, *inter alia*, a wide variety of movies,
9 television shows, and other prerecorded video materials to consumers.
10

11 **JURISDICTION AND VENUE**

12
13 23. This Court has subject-matter jurisdiction over this civil action
14 pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.
15

16 24. Personal jurisdiction and venue are proper because Defendant
17 maintains its headquarters and principal place of business in Los Angeles,
18 CA, within this judicial District.
19

20 **VIDEO PRIVACY PROTECTION ACT**

21
22 25. Generally speaking, the VPPA prohibits companies like
23 Defendant from knowingly disclosing to third parties like Meta information
24 that personally identifies consumers like Plaintiffs as having viewed
25 particular videos or other audio-visual products or services.
26
27
28

1 26. Specifically, subject to certain exceptions that do not apply here,
2 the VPPA prohibits “a video tape service provider” from “knowingly
3 disclos[ing], to any person, personally identifiable information concerning
4 any consumer of such provider[.]” 18 U.S.C. § 2710(b)(1). The statute
5 defines a “video tape service provider” as “any person, engaged in the
6 business...of rental, sale, or delivery of prerecorded video cassette tapes or
7 similar audio visual materials,” 18 U.S.C. § 2710(a)(4), and defines a
8 “consumer” as “a renter, purchaser, or subscriber of goods or services from
9 a video tape service provider.” 18 U.S.C. § 2710(a)(1). “[P]ersonally
10 identifiable information’ includes information which identifies a person as
11 having requested or obtained specific video materials or services from a
12 video tape service provider.” 18 U.S.C. § 2710(a)(3)
13
14
15
16
17

18 27. The VPPA’s purpose is as apropos today as it was at the time of
19 its enactment over 35 years ago. Leading up to the statute’s enactment in
20 1988, members of the United States Senate warned that “[e]very day
21 Americans are forced to provide to businesses and others personal
22 information without having any control over where that information goes.”
23
24 *Id.* Senators at the time were particularly troubled by disclosures of
25 records that reveal consumers’ purchases and rentals of videos and other
26
27
28

1 audiovisual materials, because such records offer “a window into our loves,
2 likes, and dislikes,” such that “the trail of information generated by every
3 transaction that is now recorded and stored in sophisticated record-
4 keeping systems is a new, more subtle and pervasive form of surveillance.”
5 S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy,
6 respectively).
7
8

9
10 28. Thus, in proposing the Video and Library Privacy Protection Act
11 (which later became the VPPA), Senator Patrick J. Leahy (the senior
12 Senator from Vermont from 1975 to 2023) sought to codify, as a matter of
13 law, that “our right to privacy protects the choice of movies that we watch
14 with our family in our own homes.” 134 Cong. Rec. S5399 (May 10, 1988).
15 As Senator Leahy explained at the time, it is the personal nature of such
16 information, and the need to protect it from disclosure, that is the *raison*
17 *d’être* of the statute: “These activities are at the core of any definition of
18 personhood. They reveal our likes and dislikes, our interests and our
19 whims. They say a great deal about our dreams and ambitions, our fears
20 and our hopes. They reflect our individuality, and they describe us as
21 people.” *Id.*
22
23
24
25
26
27
28

1 29. While these statements rang true in 1988 when the act was
2 passed, the importance of legislation like the VPPA in the modern era of
3 data mining is more pronounced than ever before. During a recent Senate
4 Judiciary Committee meeting, “The Video Privacy Protection Act:
5 Protecting Viewer Privacy in the 21st Century,” Senator Leahy emphasized
6 the point by stating: “While it is true that technology has changed over the
7 years, we must stay faithful to our fundamental right to privacy and
8 freedom. Today, social networking, video streaming, the ‘cloud,’ mobile apps
9 and other new technologies have revolutionized the availability of
10 Americans’ information.”¹

11 30. Former Senator Al Franken may have said it best: “If someone
12 wants to share what they watch, I want them to be able to do so . . . But I
13 want to make sure that consumers have the right to easily control who finds
14 out what they watch—and who doesn’t. The Video Privacy Protection Act
15 guarantees them that right.”²

16
17
18
19
20
21
22
23 ¹ The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st
24 Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the
25 Law, <http://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21stcentury>.

26 ² Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st
27 Century,
28 frank.senate.gov (Jan. 31, 2012).

1 that supports a \$26 billion dollar per year online advertising industry in
2 the United States.⁴

3
4 34. The FTC has also recognized that consumer data possesses
5 inherent monetary value within the new information marketplace and
6 publicly stated that:
7

8 Most consumers cannot begin to comprehend the
9 types and amount of information collected by
10 businesses, or why their information may be
11 commercially valuable. Data is currency. The larger
12 the data set, the greater potential for analysis – and
profit.⁵

13 35. In fact, an entire industry exists while companies known as data
14 aggregators purchase, trade, and collect massive databases of information
15 about consumers. Data aggregators then profit by selling this
16 “extraordinarily intrusive” information in an open and largely unregulated
17 market.⁶
18
19
20
21

22 ⁴ See *Web’s Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011),
23 [http://online.wsj.com/article/SB10001424052748703529004576160764037920274.ht](http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html)
ml.

24 ⁵ Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, *available at*
25 [https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-](https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf)
exploring-privacy-roundtable/091207privacyroundtable.pdf.

26 ⁶ See M. White, *Big Data Knows What You’re Doing Right Now*, TIME.com (July
27 31, 2012), [http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-](http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/)
right-now/.

1 36. The scope of data aggregators' knowledge about consumers is
 2 immense: "If you are an American adult, the odds are that [they] know[]
 3 things like your age, race, sex, weight, height, marital status, education
 4 level, politics, buying habits, household health worries, vacation dreams—
 5 and on and on."⁷

6
 7
 8 37. Further, "[a]s use of the Internet has grown, the data broker
 9 industry has already evolved to take advantage of the increasingly specific
 10 pieces of information about consumers that are now available."⁸

11
 12 38. Recognizing the serious threat the data mining industry poses
 13 to consumers' privacy, on July 25, 2012, the co-Chairmen of the
 14 Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data
 15 brokerage companies seeking information on how those companies collect,
 16 store, and sell their massive collections of consumer data, stating in
 17 pertinent part:

18
 19 By combining data from numerous offline and online
 20 sources, data brokers have developed hidden

21
 22
 23 ⁷ N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y.
 24 Times (June 16, 2012), *available at*
[http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-](http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html)
 25 [consumer-database-marketing.html](http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html).

26 ⁸ Letter from Sen. J. Rockefeller IV, Sen. Cmtee. on Commerce, Science, and
 27 Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) *available*
 28 *at* [http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-](http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-4157-a97b-a658c3c3061c)
[4157-a97b-a658c3c3061c](http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-4157-a97b-a658c3c3061c).

1 dossiers on every U.S. consumer. This large[-]scale
2 aggregation of the personal information of hundreds
3 of millions of American citizens raises a number of
4 serious privacy concerns.⁹

5 39. Data aggregation is especially troublesome when consumer information
6 is sold to direct-mail advertisers. In addition to causing waste and inconvenience,
7 direct-mail advertisers often use consumer information to lure unsuspecting
8 consumers into various scams,¹⁰ including fraudulent sweepstakes, charities, and
9 buying clubs. Thus, when companies like Shout! Factory, LLC share information
10 with data aggregators, data cooperatives, and direct-mail advertisers, they contribute
11 to the “[v]ast databases” of consumer data that are often “sold to thieves by large
12 publicly traded companies,” which “put[s] almost anyone within the reach of
13 fraudulent telemarketers” and other criminals.¹¹

14 40. Disclosures like Defendant’s are particularly dangerous to the
15 elderly. “Older Americans are perfect telemarketing customers, analysts
16 say, because they are often at home, rely on delivery services, and are
17 say, because they are often at home, rely on delivery services, and are
18 say, because they are often at home, rely on delivery services, and are
19 say, because they are often at home, rely on delivery services, and are
20 say, because they are often at home, rely on delivery services, and are
21 say, because they are often at home, rely on delivery services, and are

22 ⁹ See *Bipartisan Group of Lawmakers Query Data Brokers About Practices*
23 *Involving Consumers’ Personal Information*, Website of Sen. Markey (July 24, 2012),
24 [http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-](http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information)
25 [brokers-about-practices-involving-consumers-personal-information](http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information).

26 ¹⁰ See *Prize Scams*, Federal Trade Commission
27 <http://www.consumer.ftc.gov/articles/0199-prize-scams> (last visited July 30, 2021).

28 ¹¹ See Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times, May
29 20, 2007, available at <http://www.nytimes.com/2007/05/20/business/20tele.html> (last
30 visited July 30, 2021).

1 lonely for the companionship that telephone callers provide.”¹² The FTC
2 notes that “[t]he elderly often are the deliberate targets of fraudulent
3 telemarketers who take advantage of the fact that many older people have
4 cash reserves or other assets to spend on seemingly attractive offers.”¹³
5

6
7 41. Indeed, an entire black market exists while the personal
8 information of vulnerable elderly Americans is exchanged. Thus,
9 information disclosures like Defendant’s are particularly troublesome
10 because of their cascading nature: “Once marked as receptive to [a specific]
11 type of spam, a consumer is often bombarded with similar fraudulent offers
12 from a host of scam artists.”¹⁴
13

14
15 42. Defendant is not alone in violating its customers’ statutory
16 rights and jeopardizing their well-being in exchange for increased revenue:
17 disclosing customer and subscriber information to data aggregators, data
18 appenders, data cooperatives, direct marketers, and other third parties has
19 become a widespread practice. Unfortunately for consumers, however, this
20 growth has come at the expense of their most basic privacy rights.
21
22
23

24 ¹² *Id.*

25 ¹³ *Fraud Against Seniors: Hearing before the Senate Special Committee on Aging*
26 (August 10, 2000) (prepared statement of the FTC), available at
27 [https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-](https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-fraud-against-seniors/agingtestimony.pdf)
statement-federal-trade-commission-fraud-against-seniors/agingtestimony.pdf.

28 ¹⁴ *Id.*

II. Consumers Place Monetary Value on their Privacy and Consider Privacy Practices When Making Purchases

43. As the data aggregation industry has grown, so too have consumer concerns regarding their personal information.

44. A recent survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies who they believe do not protect their privacy online.¹⁵ As a result, 81 percent of smartphone users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.¹⁶

45. Thus, as consumer privacy concerns grow, consumers are increasingly incorporating privacy concerns and values into their purchasing decisions and companies viewed as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy- protective competitors.

¹⁵ See 2014 TRUSTe US Consumer Confidence Privacy Report, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

¹⁶ *Id.*

1 46. In fact, consumers' personal information has become such a
 2 valuable commodity that companies are beginning to offer individuals the
 3 opportunity to sell their personal information themselves.¹⁷

5 47. These companies' business models capitalize on a fundamental
 6 tenet underlying the personal information marketplace: consumers
 7 recognize the economic value of their private data. Research shows that
 8 consumers are willing to pay a premium to purchase services from
 9 companies that adhere to more stringent policies of protecting their
 10 personal data.¹⁸

14 48. Thus, in today's digital economy, individuals and businesses
 15 alike place a real, quantifiable value on consumer data and corresponding
 16 privacy rights.¹⁹ As such, where a business offers customers a service that

17 ¹⁷ See Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal*
 20 *Data*, N.Y. Times (Feb. 12, 2012), available at
 21 <http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html>.

22 ¹⁸ See Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy*
 23 *Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254
 24 (2011); see also European Network and Information Security Agency, *Study on*
 25 *monetising privacy* (Feb. 27, 2012), available at
 26 <https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy>.

27 ¹⁹ See Hann, et al., *The Value of Online Information Privacy: An Empirical*
 28 *Investigation* (Oct. 2003) at 2, available at
 29 <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.321.6125&rep=rep1&type=pdf> ("It is obvious that people value online privacy.").

1 includes statutorily guaranteed privacy protections, yet fails to honor these
2 guarantees, the customer receives a service of less value than the service
3 paid for.
4

5 **III. Defendant Uses the Meta Pixel to Systematically Disclose**
6 **its Customers' Personal Viewing Information to Meta**

7 49. As alleged below, when a customer of any of Defendant's
8 websites purchases a specific video, the Meta Pixel technology that
9 Defendant intentionally installed on its websites transmits the customer's
10 personally identifying information and detailed information concerning the
11 specific interactions the customer takes on its websites (including the
12 customer's Private Viewing Information revealing the specific videos that
13 he or she purchased) to Meta, without the customer's consent and in clear
14 violation of the VPPA.
15
16
17

18 **A. The Meta Pixel**
19

20 50. On February 4, 2004, Mark Zuckerberg and others launched
21 Facebook, now known as "Meta".²⁰ Since then, Meta has become the world's
22 largest social media platform. To create a Meta account, a person must
23 provide, *inter alia*, his or her first and last name, birthdate, gender, and
24 phone number or email.
25
26

27 _____
28 ²⁰ Company Info, FACEBOOK, <https://about.fb.com/company-info>

1 51. The Meta Pixel, first introduced in 2013 as the “Facebook Pixel,”
2
3 is a unique string of code that companies can embed on their websites to
4 allow them to track consumers’ actions and report the actions back to Meta.

5 52. The Meta Pixel allows online-based companies like Defendant
6
7 to build detailed profiles about their visitors by collecting information about
8 how they interact with their websites, and to then use the collected
9
10 information to service highly targeted advertising to them.

11 53. Additionally, a Meta Pixel installed on a company’s website
12
13 allows Meta “to match . . . website visitors to their respective [Meta] User
14 accounts.”²¹ Meta is able to do this because it has assigned to each of its
15 users an “FID” number – a unique and persistent identifier that allows
16
17 anyone to look up the user’s unique Meta profile and thus identify the user
18 by name²² – and because each transmission of information made from a
19 company’s website to Meta via the Meta Pixel is accompanied by, *inter alia*,
20
21 the FID of the website’s visitor. Moreover, the Meta Pixel can follow a
22

23
24 ²¹ <https://developers.facebook.com/docs/meta-pixel/get-started>.

25 ²² For example, Mark Zuckerberg’s FID is reportedly the number “4,” so logging
26 into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark
27 Zuckerberg’s Facebook page: www.facebook.com/zuck, and all of the additional
28 personally identifiable information contained therein.

1 consumer to different websites and across the Internet even after clearing
2 browser history.
3

4 54. Meta has used the Meta Pixel to amass a vast digital database
5 of dossiers comprised of highly detailed personally identifying information
6 about each of its billions of users worldwide, including information about
7 all of its users' interactions with any of the millions of websites across the
8 Internet on which the Meta Pixel is installed. Meta then monetizes this
9 Orwellian database by selling advertisers the ability to serve highly
10 targeted advertisements to the persons whose personal information is
11 contained within it.
12
13
14

15 55. Simply put: if a company chooses to install the Meta Pixel on its
16 website, both the company who installed it and Meta (the recipient of the
17 information it transmits) are then able to "track[] the people and type of
18 actions they take"²³ on the company's website, including the purchases they
19 made, the items they spent time viewing, and, as relevant here, the specific
20 video content that they purchased on the website.
21
22
23
24
25

26 **B. Defendant Knowingly Uses the Meta Pixel to Transmit the**

27 ²³ <https://www.facebook.com/business/goals/retargeting>.
28

1 **Private Viewing Information of its Customers to Meta**

2 56. To purchase video products from Defendant's websites, the
3
4 consumer must provide at least his or her name, email address, billing
5 address, and credit- or debit card (or other form of payment) information.
6

7 57. After a person has completed the order process on Defendant's
8 websites, Defendant uses – and has used at all times relevant hereto – the
9 Meta Pixel to disclose to Meta the unencrypted FID of the customer and
10 the specific videos that he or she purchased from Defendant's websites.
11

12 58. Defendant intentionally programmed its websites (by following
13 step-by-step instructions from Meta's website) to include a Meta Pixel that
14 systematically transmits to Meta the FIDs of its customers and the video
15 products that each of them requested in order to take advantage of the
16 targeted advertising and other informational and analytical services
17 offered by Meta.
18
19
20

21 59. With only a person's FID and the video content name or URL
22 that the person requested on Defendant's websites—all of which Defendant
23 knowingly provides to Meta —any ordinary person could learn the identity
24 of the person to whom the FID corresponds and the specific video products
25 or services that this person requested. This can be accomplished simply by
26
27
28

1 accessing the URL [www.facebook.com/\[unencrypted FID/\]](http://www.facebook.com/[unencrypted FID/]).

2
3 60. Defendant's practices of disclosing the Private Viewing
4 Information of its customers to Meta continued unabated for the full
5 duration of the time period relevant to this action. At all times relevant
6 hereto, whenever Plaintiffs or another customer of Defendant's websites
7 purchased a particular video from Defendant's websites, Defendant
8 disclosed to Meta that (*inter alia*) the specific video that was purchased
9 (including the URL where such video was purchased), along with the FID
10 of the customer who requested it (which, as discussed above, uniquely
11 identifies the person).

12
13
14
15 61. At all relevant times, Defendant knew that the Meta Pixel
16 disclosed its customers Private Viewing Information to Meta.

17
18 62. Defendant could easily have programmed its websites so that
19 none of its customers' detailed Private Viewing Information is disclosed to
20 Meta. Instead, Defendant chose to program its websites so that all of its
21 customers' detailed Private Viewing Information is sent to Meta *en masse*.

22
23 63. Prior to transmitting its customers' Private Viewing
24 Information to Meta, Defendant failed to notify Plaintiffs or any of its other
25 customers that it would do so, and neither Plaintiffs nor any of its other
26
27

1 customers have consented (in writing or otherwise) to these practices.

2
3 64. By intentionally disclosing to Meta Plaintiffs' and its other
4 customers' FIDs together with the specific video content they each
5 purchased, without Plaintiffs' or any of its other customers' consent to these
6 practices, Defendant knowingly and systematically violated the VPPA on
7 an enormous scale.
8

9
10 **CLASS ACTION ALLEGATIONS**

11 65. Plaintiffs seeks to represent a class defined as all persons in the
12 United States who, during the two years preceding the filing of this action,
13 purchased video content from Defendant's websites as a consumer of
14 Defendant's websites and while maintaining an account with Meta
15 Platforms, Inc. f/k/a Facebook, Inc.
16
17

18 66. Class members are so numerous that their individual joinder
19 herein is impracticable. On information and belief, members of the Class
20 number in at least the tens of thousands. The precise number of Class
21 members and their identities are unknown to Plaintiffs at this time but
22 may be determined through discovery. Class members may be notified of
23 the pendency of this action by mail and/or publication through the
24 membership records of Defendant.
25
26
27
28

1 67. Common questions of law and fact exist for all Class members
2 and predominate over questions affecting only individual class members.
3
4 Common legal and factual questions include, but are not limited to: (a)
5 whether Defendant knowingly disclosed Plaintiffs' and Class members'
6 Private Viewing Information to Meta; (b) whether Defendant's conduct
7 violates the Video Privacy Protection Act, 18 U.S.C. § 2710; (c) whether
8 Defendant should be enjoined from disclosing Plaintiffs' and Class
9 members' Private Viewing Information to Meta; and (d) whether Plaintiffs
10 and Class members are entitled to statutory damages for the
11
12 aforementioned violations.
13
14

15 68. The named Plaintiffs' claims are typical of the claims of the
16 Class in that the named Plaintiffs and the Class members suffered
17
18 invasions of their statutorily protected right to privacy (as afforded by the
19 VPPA), as well as intrusions upon their private affairs and concerns that
20
21 would be highly offensive to a reasonable person, as a result of Defendant's
22 uniform and wrongful conduct in intentionally disclosing their Private
23 Purchase Information to Meta.
24

25 69. Plaintiffs are adequate representatives of the Class because
26 their interests do not conflict with the interests of the Class members they
27
28

1 seek to represent, they have retained competent counsel experienced in
2 prosecuting class actions, and they intend to prosecute this action
3 vigorously. Plaintiffs and their counsel will fairly and adequately protect
4 the interests of Class members.
5

6
7 70. The class mechanism is superior to other available means for
8 the fair and efficient adjudication of Class members' claims. Each
9 individual Class Member may lack the resources to undergo the burden and
10 expense of individual prosecution of the complex and extensive litigation
11 necessary to establish Defendant's liability. Individualized litigation
12 increases the delay and expense to all parties and multiplies the burden on
13 the judicial system presented by this case's complex legal and factual
14 issues. Individualized litigation also presents a potential for inconsistent
15 or contradictory judgments. In contrast, the class action device presents
16 far fewer management difficulties and provides the benefits of single
17 adjudication, economy of scale, and comprehensive supervision by a single
18 court on the issue of Defendant's liability. Class treatment of the liability
19 issues will ensure that all claims and claimants are before this Court for
20 consistent adjudication of the liability issues.
21
22
23
24
25

26
27 **CAUSE OF ACTION**
28 **Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710**

1
2 71. Plaintiffs repeat the allegations asserted in the preceding
3 paragraphs as if fully set forth herein.

4
5 72. Plaintiffs bring their claims individually and on behalf of the
6 putative Class Members against Defendant.

7
8 73. The VPPA prohibits a “video tape service provider” from
9 knowingly disclosing “personally identifying information” concerning any
10 “consumer” to a third-party without the “informed, written consent
11 (including through an electronic means using the Internet) of the
12 consumer.” 18 U.S.C. § 2710.

13
14 74. As defined in 18 U.S.C. § 2710(a)(4), a “video tape service
15 provider” is “any person, engaged in the business, in or affecting interstate
16 or foreign commerce, of rental, sale, or delivery of prerecorded video
17 cassette tapes or similar audiovisual materials[.]” Defendant is a “video
18 tape service provider” as defined in 18 U.S.C. § 2710(a)(4) because it is
19 engaged in the business of delivering audiovisual materials that are similar
20 to prerecorded video cassette tapes and those sales affect interstate or
21 foreign commerce.
22

23 75. As defined in 18 U.S.C. § 2710(a)(1), a “consumer” means any
24 renter, purchaser, or consumer of goods or services from a video tape service
25
26
27
28

1 provider.” As alleged above, Plaintiffs and Class members are consumers to
2 Defendant’s service of providing video content. Thus, Plaintiffs and Class
3 members are “consumers” under this definition.
4

5 76. As defined in 18 U.S.C. § 2710(a)(3), “‘personally identifiable
6 information’ includes information which identifies a person as having
7 requested or obtained specific video materials or services from a video tape
8 service provider.”
9

10
11 77. Defendant knowingly disclosed Plaintiffs’ and Class members’
12 Private Viewing Information to Meta in the manner alleged herein.
13

14 78. The Private Viewing Information that Defendant transmitted to
15 Meta constitutes personally identifiable information under 18 U.S.C. §
16 2710(a)(3) because it identified Plaintiffs and each Class member to Meta
17 as an individual who purchased video content, including the specific video
18 materials purchased from Defendant’s websites.
19

20
21 79. Defendant never obtained informed, written consent from
22 Plaintiffs or any Class member to disclose their Private Viewing
23 Information to Meta or any other third party. More specifically, Defendant
24 never obtained from Plaintiffs or any Class member informed, written
25 consent in a form distinct and separate from any form setting forth other
26
27
28

1 legal or financial obligations of the consumer; Defendant never obtained
2 from Plaintiffs or any Class member informed, written consent that, at the
3 election of the consumer, was given at the time the disclosure is sought or
4 was given in advance for a set period of time, not to exceed two years or
5 until consent is withdrawn by the consumer, whichever is sooner; and
6 Defendant never provided an opportunity, in a clear and conspicuous
7 manner, for Plaintiffs or any Class member to withdraw consent on a case-
8 by-case basis or to withdraw consent from ongoing disclosures, at the
9 consumer's election. *See* 18 U.S.C. § 2710(b)(2).
10
11
12
13

14 80. Defendant knowingly disclosed such information to Meta
15 because Defendant intentionally installed and programmed the Meta Pixel
16 code on its website, knowing that such code would transmit to Meta the
17 video titles requested by its customers and its customers' unique identifiers
18 (including FIDs) when customers purchased videos from its website.
19
20

21 81. By disclosing Plaintiffs' and Class members' Private Viewing
22 Information, Defendant violated their statutorily protected right to privacy
23 in the videos they purchased from Defendant. 18 U.S.C. § 2710(c).
24

25 82. As a result of these violations, Defendant is liable to Plaintiffs
26 and Class members for damages and other relief as provided by the VPPA.
27
28

1 83. On behalf of themselves and all members of the Class, Plaintiffs
2 seek to enjoin Defendant's future disclosures of its customers' Private
3 Viewing Information; liquidated damages in the amount of \$2,500 per
4 violation of the VPPA; reasonable attorneys' fees and costs; and all other
5 preliminary or equitable relief the Court deems appropriate. 18 U.S.C. §
6 2710(c)(2)(A).
7

8
9
10 **PRAYER FOR RELIEF**

11 WHEREFORE, Plaintiffs, individually and on behalf of all others
12 similarly situated, seeks a judgment against Defendant Shout! Factory
13 LLC as follows:
14

- 15 A. For an order certifying the Class under Rule 23 of the
16 Federal Rules of Civil Procedure and naming
17 Plaintiffs as representatives of the Class and
18 Plaintiffs' attorneys as Class Counsel to represent the
19 Class;
20 B. For an order declaring that Defendant's conduct as
21 described herein violated the VPPA;
22 C. For an order finding in favor of Plaintiffs and the
23 Class and against Defendant on all counts asserted
24 herein;
25 D. For an award of \$2,500.00 to the Plaintiffs and each
26 Class member, as provided by the VPPA, 18 U.S.C. §
27 2710(c);
28

- 1 E. For an order permanently enjoining Defendant from
2 disclosing the Private Viewing Information of its
3 customers to third parties in violation of the VPPA.
- 4 F. For prejudgment interest on all amounts awarded;
5 and
- 6 G. For an order awarding punitive damages, reasonable
7 attorneys' fees, and costs to counsel for Plaintiffs and
8 the Class under Rule 23 and 18 U.S.C. § 2710(c).

9 **JURY DEMAND**

10 Plaintiffs demand a trial by jury on all causes of action and issues so
11 triable.
12

13
14
15 Dated: August 20, 2024

Respectfully submitted,

16
17 /s/ Frank S. Hedin

18 **HEDIN LLP**

19 FRANK S. HEDIN

20 535 Mission Street, 14th Floor

San Francisco, CA 94105

21 TELEPHONE: (305) 357-2107

22 FACSIMILE: (305) 200-8801

23 FHEDIN@HEDINLLP.COM

24 *Counsel for Plaintiff and Putative Class*
25
26
27
28